#9
KWS
6-5-03

1of3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Attorney Docket No. **RP9-99-048**

In re Application of:	§	
	§	
CROMER ET AL.	§	
	§	Examiner: **LEE, C.**
Serial No. **09/281,852**	§	
	§	Art Unit: **2131**
Filed: **31 MARCH 1999**	§	
	§	
For: **DATA PROCESSING SYSTEM AND METHOD FOR MAINTAINING SECURE DATA BLOCKS**	§	
	§	
	§	

APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief is submitted in triplicate in support of the Appeal in the above-identified application.

CERTIFICATE OF MAILING
37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as First-Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date below.

5-27-03
Date

Kathy Schoen
Signature

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, the real party of interest.

RELATED APPEALS AND INTERFERENCES

No related appeal is presently pending.

STATUS OF THE CLAIMS

Claims 1-7 and 10-16 stand finally rejected by the Examiner as noted in the Final Office Action dated April 9, 2003 and the Advisory Action dated May 12, 2003.

STATUS OF AMENDMENTS

No amendment was submitted subsequent to the Office Action dated 8 January, 2003.

SUMMARY OF THE INVENTION

With the proliferation of online services via the Internet, there is a tremendous need to identify and authenticate Internet users for security reasons. Before an Internet user is permitted to access a secure website, the Internet user is typically required to provide a username and a corresponding password. In order to provide more efficient access to various websites, an Internet service may provide a block of data, commonly known as a *cookie*, to a user computer system. The cookie may include public information pertaining to the Internet service and private information associated with the user. For example, a cookie may include, *inter alia*, a username and a corresponding password, the user's credit card information, the user's address, and the user's online usage preferences. Because it is paramount to maintain the data security of cookies when private and sensitive information are involved, it is most preferable to store cookies in a secure storage area of a computer system.

Over time, a single user may have many cookies stored on his/her computer system. It is most likely that the number of cookies will eventually exceed the storage size of a secure storage area within a typical computer system. But if the "overflow" cookies are stored in a non-secured storage area of a computer system, such as a hard disk drive, it is foreseeable that an unauthorized user can copy a user's cookies from the user's computer system to another computer system for the purpose of extracting valuable information stored within the cookies. Therefore, it is desirable to provide a method for storing cookies in a non-secured mass storage device without sacrificing the data security of the cookies.

In accordance with a preferred embodiment of the present invention, an encryption key pair, which includes a private key and a public key, is stored in a protected storage device within a data processing system, as shown in block **304** of Figure **3**. In response to the receipt of a cookie generated by an application from a remote server, the cookie is encrypted with the public key of the encryption key pair, as depicted in block **308** of Figure **3**. The encrypted cookie can now be stored in a non-protected storage device, such as a hard disk drive, within the data processing system, as shown in block **310** of Figure **3**. In response to an access request for the encrypted cookie by a browser program executing within the data processing system, a copy of the encrypted cookie is sent to the protected storage device, as depicted in block **408** of Figure **4**, and the encrypted cookie is decrypted using the private key within the protected storage device, as shown in block **410** of Figure **4**. Finally, the decrypted cookie is sent to the browser program requesting the cookie, as shown in block **412** of Figure **4**.

ISSUE

Is the Examiner's rejection of Claims 1-7 and 10-16 under 35 U.S.C. § 103(a) as being unpatentable over *Paltenghe et al.* (US 6,421,729) in view of *Pond et al.* (US 4,864,616) and *Schneier*, Applied Cryptography, 2nd ed., John Wiley & Sons, Inc., 1996 well-founded?

GROUPING OF THE CLAIMS

For purposes of this Appeal, Claims 1-7 and 10-16 stand or fall together as a single group.

ARGUMENT

The Examiner's rejections of Claims 1-7 and 10-16 are not well-founded and should be reversed.

I. The motivations of *Paltenghe* and *Pond* are so divergent that they cannot be reconciled for the purpose of obviousness rejection

Claim 1 (and similarly Claim 10) recites steps of "in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key" (lines 5-6), "storing said encrypted cookie in a non-protected storage device within said data processing system" (lines 7-8), "in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key" (lines 9-11) and "sending said decrypted cookie to said browser program" (line 12).

Thus, according to the claimed invention, a cookie generated by a software application from a remote server is encrypted by a public key of a public-private encryption key pair before the cookie is stored in a non-protected storage device. When the encrypted cookie is being requested by a browser program, the encrypted cookie is then decrypted by a private key of the public-private encryption key pair before sending to the browser program. As such, a cookie can be securely stored in a non-protected storage device of a data processing system.

On page 3 of the Final Office Action, the Examiner states that "Paltenghe does not expressly disclose a) a protected storage device for storing a[sic] encryption key pair; b) means for utilizing public key to encrypt cookie before storing it to the hard disk; c) means for utilizing private key to decrypt cookie." The reason that *Paltenghe* does not disclose any encryption of cookies is because *Paltenghe* was never concerned about the data security of the cookies. In fact, according to *Paltenghe*, cookies are simply stored in the hard drive of a user's computer system in the form a plain text file (col. 6, line 60-62), which is indicative of the fact that *Paltenghe*'s motivation did not lie upon data security of the cookies. This is contrary to the Examiner's assertion on page 2 of the Advisory Action that "the cookie is an obvious important information in the Paltenghe et al, it would have been obvious to encrypt it in the hard disk."

Under MPEP § 706.02(j), in order to establish a *prima facie* case of obviousness, three criteria must be met. First, there must be some suggestion or motivation to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Third, the prior art reference(s) must teach or suggest all the claimed limitations. In the present case, the Examiner has not provided any reason or motivation for combining the teachings of *Paltenghe*, *Pond* and *Schneier.*

On page 2 of the Advisory Action, the Examiner asserts that such motivation comes from *Pond.* The Examiner further explains that *Pond* suggests a motivation for encrypting an important file in a hard drive is to provide a high level of protection even if the hard drive is physically stolen. Since *Paltenghe* has indicated that data security of cookies is not a concern, as mentioned above; thus, *Paltenghe*'s teaching is apparently in direct conflict with the motivation for encryption as disclosed by *Pond.* When there is a conflict between the teachings of two or more prior art references, under MPEP § 2143.01, "the Examiner <u>must</u> weigh the power of each reference to suggest solutions to one of ordinary skill in the art, considering the degree to which one reference might accurately discredit another" (emphasis added). The Examiner has neglected to do so in the Final Office Action and the Advisory Action. Furthermore, since *Paltenghe* is the primary reference, any reason or motivation for modifying the teachings of *Paltenghe* should come from *Paltenghe* itself instead of from the secondary reference *Pond.* Hence, it is apparent that the motivations of *Paltenghe* and *Pond* are so different that they cannot be reconciled for the purpose of obviousness rejection.

<u>II. The cited references do not teach or suggest the claimed encrypting and decrypting steps</u>

Even though both *Pond* and *Schneier* are related to cryptography, neither *Pond* nor *Schneier* teaches or suggests the claimed steps of "encrypting said cookie with said public key" and "decrypting said encrypted cookie with said private key." On page 2 of the Advisory Action, the Examiner asserts that the claimed encrypting and decrypting steps are disclosed by *Pond* in col. 6, lines 35-63. However, col. 6, lines 35-63 of *Pond* teaches that data entered into a protected file is first encrypted under a Mandatory Key Stream **20** and then under each of the other key streams designated by a Key Mix **36**. *Pond* further explains that based on Key Mix **36** designated during the creation of the protected file, the file can only be decrypted under one of the four conditions listed in col. 6, lines 45-54. There is no teaching or suggestion in *Pond* as to the claimed "encrypting said cookie with said public key" and "decrypting said encrypted cookie with said private key." Because the cited references, whether considered separately or in combination, do not teach or suggest the claimed invention, the § 103 rejection is improper.

CONCLUSION

For the reasons stated above, Appellants believe that the claimed invention clearly is patentably distinct over the cited references and that the rejections under 35 U.S.C. § 103 are not well-founded. Hence, Appellants respectfully urge the Board to reverse the Examiner's rejection.

Please charge the IBM Deposit Account **50-0563** in the amount of $320.00 for submission of a Brief in support of Appeal. No additional fee or extension of time is believed to be required; however, in the event an additional fee or extension of time is required, please charge that fee or extension of time requested to the IBM Deposit Account **50-0563**.

Respectfully submitted,

Antony P. Ng
Registration No. 43,427
BRACEWELL & PATTERSON, LLP
111 Congress Avenue, Suite 2300
Austin, Texas 78701
512.542.2134

ATTORNEY FOR APPELLANTS

APPENDIX

1. A method for protecting the security of a cookie stored within a data processing system, said method comprising:

storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system;

in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key;

storing said encrypted cookie in a non-protected storage device within said data processing system;

in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key; and

sending said decrypted cookie to said browser program.

2. The method according to claim 1, wherein said non-protected storage device is a hard drive.

3. The method according to claim 1, further comprising providing an encryption device having an encryption engine and said protected storage device accessible only through said encryption engine.

4. The method according to claim 3, wherein said encrypting further include encrypting said cookie utilizing said encryption device.

5. The method according to claim 4, wherein said decrypting further includes decrypting said encrypted cookie utilizing said encryption device.

6. The method according to claim 5, wherein said sending further includes transmitting said decrypted cookie from said encryption device to said browser program.

7. The method according to claim 6, further comprising transmitting said decrypted cookie from said browser program to an application executing in a remote server.

10. A data processing system capable of protecting the security of a cookie stored within said data processing system, said data processing comprising:

a protected storage device for storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system;

means for utilizing said public key to encrypt said cookie, in response to the receipt of a cookie generated by an application from a remote server;

a non-protected storage device within said data processing system for storing encrypted cookie;

means for utilizing said private key to decrypt said encrypted cookie, in response to an access request for said encrypted cookie by a browser program executing within said data processing system; and

means for sending said decrypted cookie to said browser program.

11. The data processing system according to claim 10, wherein said non-protected storage device is a hard drive.

12. The data processing system according to claim 10, further comprising an encryption device having an encryption engine and said protected storage device accessible only through said encryption engine.

13. The data processing system according to claim 12, wherein said means for utilizing said public key to encrypt said cookie is said encryption engine.

14. The data processing system according to claim 13, wherein said means for utilizing said private key to decrypt said encrypted cookie is said encryption device.

15. The data processing system according to claim 14, wherein said sending means further includes means for transmitting said decrypted cookie from said encryption device to said browser program.

16. The data processing system according to claim 15, further comprising means for transmitting said decrypted cookie from said browser program to an application executing in a remote server.